UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

UNITED STATES OF AMERICA,
***ex rel.* JEFFREY BROOKS,**

Plaintiff,

V.

CITY LIGHT AND POWER, INC.,

Defendants

Case No.:

Jury Trial Demanded

Filed Under Seal
31 U.S.C. § 3730(b)(2)

COMPLAINT

Claims Pursuant to the False Claims Act, 31 USC sec. 3729, *et seq.*

[FILED IN CAMERA AND UNDER SEAL]

UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

UNITED STATES OF AMERICA,
***ex rel.* JEFFREY BROOKS,**

Case No.:

Plaintiffs,

V.

CITY LIGHT AND POWER, INC.,

Jury Trial Demanded

Filed Under Seal
31 U.S.C. § 3730(b)(2)

Defendant.

COMPLAINT
Claims Pursuant to the False Claims Act, 31 USC sec. 3729, *et seq.*

SUMMARY INTRODUCTION

1. The United States of America, by and through *qui tam* originating Relator, Jeffrey Brooks ("Relator" or "Brooks"), hereby brings this action pursuant to the False Claims Act ("FCA"), as amended, 31 U.S.C. § 3729 et seq., by and through his attorneys, Brian H. Mahany and the Law Firm of MAHANY LAW and David P. Weber and Richard J. Link of GOODWIN WEBER PLLC, and hereby declares the following to recover all damages, penalties, and other remedies available as established by the FCA that were caused by Defendant's creation of false and deceptive records, billings, statements, reports and omission of facts relied upon by the United States Government in the awarding of numerous governmental contracts and issuing payments to Defendant upon the same.

2. As set forth in detail below, City Light and Power, Inc. ("CLP") bid upon and ultimately was awarded numerous governmental contracts for the supply and maintenance of electrical distribution and infrastructure services and supplies to U.S. military installations. Pursuant to various provisions of the Federal Acquisition Regulation, Defense Federal Acquisition Regulation and the Homeland Security Acquisition Regulation, CLP was commanded to undertake certain security measures to safeguard information systems operated and/or maintained pursuant to government contracts, the governmental information received from governmental entities maintained on or transiting thorough such information systems and to timely report to government officials breaches of these required security measures. Nevertheless, CLP has knowingly, willfully and repeatedly failed or otherwise refused to undertake these required security and reporting requirements while continuing to create and submit claims to the United States for payment and approval, and upon which the United States has and continues to make payment.

THE PARTIES

3. Plaintiff is the United States of America.

4. Relator is a citizen of the State of Colorado and former Systems Administrator and Junior Database Administrator for CLP via contract with Robert Half Technology from March 30 of 2016 through August 12 of 2016. In that position, Brooks' duties included, among other things, the examination of software and information systems for the discovery of system security updates necessary to avoid cyber intrusion into information systems operated and maintained pursuant to contracts with the United States. It was during his employment with CLP that Brooks became the original source of the information contained herein and witnessed the conduct, actions and inactions alleged in this Complaint.

5. City Light and Power, Inc. ("CLP"), upon information and belief, is a citizen Corporation of the State of Nevada, organized and existing under the laws of the State of Nevada with corporate offices located in both California at 2961 Rodondo Avenue in Long Beach, California, 90806 and in Colorado at 6312 South Fiddlers Green Circle, Suite 200E, Greenwood Village, CO 80111. The registered agent for service of process for City light and Power, Inc. in Nevada is Resident Agents of Nevada, Inc., located at 711 South Carson Street, Suite 4, in Carson City, Nevada 89701. Upon further information and belief, CLP has conducted, and continues to carry on business activities throughout the United States, including upon military installations located in the States of Maryland, California and Utah.

JURISDICTION AND VENUE

6. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 and 31 U.S.C. § 3732, the latter of which specifically confers jurisdiction on this Court for actions brought pursuant to 31 U.S.C. §§ 3729 and 3730. Plaintiff-Relator establishes subject matter jurisdiction under 31 U.S.C. § 3730(b).

7. This Court has personal jurisdiction over the Defendant as a citizen domiciled in this jurisdiction and this is a proper venue pursuant to 28 U.S.C. § 1391(b) and 31 U.S.C. § 3732(a). Moreover, the Defendant has and continues to conduct business throughout the United States, including this jurisdiction.

FEDERAL FALSE CLAIMS ACT

8. The False Claims Act, 31 U.S.C. §§ 3729-3733, provides, *inter alia*, that any person who: (1) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval, or (2) knowingly makes, uses, or causes to be made or used, a false record or statement

material to a false or fraudulent claim, is liable to the United States for a civil monetary penalty plus treble damages. 31 U.S.C. § 3729(a)(1)(A)-(B).

9. The statute also provides liability for anyone that conspires to violate a provision (A)-(G) of the False Claims Act. 31 U.S.C. §3729(a)(1)(C).

10. The False Claims Act defines the term "claim" to mean "any request or demand, whether under a contract or otherwise, for money or property and whether or not the United States has title to the money or property, that: (i) is presented to an officer, employee, or agent of the United States; or (ii) is made to a contractor, grantee, or other recipient, if the money or property is to be drawn down or used on the Government's behalf or to advance a Government program or interest, and if the United States Government: (i) provides or has provided any portion of the money or property requested or demanded; or (ii) will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded...." 31 U.S.C. § 3729(b)(2)(A) (2009).

11. The terms "knowing" and "knowingly" are defined to mean "that a person, with respect to information: (1) has actual knowledge of the information; (2) acts in deliberate ignorance of the truth or falsity of the information; or (3) acts in reckless disregard of the truth or falsity of the information." 31 U.S.C. § 3729(b)(1)(A)(i)-(iii). Proof of specific intent to defraud is not required. 31 U.S.C. § 3729(b)(1)(B).

12. As utilized within the False Claims Act, "the term 'material' means having a natural tendency to influence, or capable of influencing, the payment or receipt of money or property." 31 U.S.C. § 3729(b)(4).

13. Private citizens are encouraged to bring actions on behalf of the government pursuant to 31 U.S.C. § 3730(b)(1), which states, "[a] person may bring a civil action for a violation

of section 3729 for the person and for the United States Government. The action shall be brought in the name of the Government." 31 U.S.C. § 3730(b)(1).

14. Pursuant to 31 U.S.C. § 3730(e), there has been no statutory relevant public disclosure of the allegations or transactions referenced in this Complaint to which Plaintiff-Relator Brooks is not the "original source," and all material information relevant to this Complaint is being provided to the United States Government in accord with 31 U.S.C. § 3730(e)(4)(B).

15. The United States, through Relator, herein alleges that CLP has violated and continues to violate the foregoing provisions of the FCA by seeking payment for the installation and monitoring of electrical infrastructure equipment, information systems and security measures in accordance with the requirements of its contracts with the Department of Defense ("DOD"), the Defense Logistics Agency ("DLA"), the Department of the Air Force ("DOAF") and the Department of the Army ("DOA"), when CLP knew the contractually required security maintenance, analysis and software updates were not occurring and had not occurred for significant periods of time, and that CLP failed comply with mandatory reporting periods relating to cyber security intrusions of the same. Due to CLP's fraudulent conduct, the DOD, DLA, DOAF and DOA accepted and paid for the installation and maintenance of electrical and information system security they would not otherwise have accepted or paid for had they known the truth of CLP's actions and inactions.

GOVERNMENT CONTRACTING AUTHORITY AND CONTROLLING REGULATIONS FOR ELECTRIC POWER DISTRIBUTION

16. Per the Congressional Research Center in 2011, the federal government purchases roughly 57 million megawatt-hours of electricity annually, making it the single largest U.S. energy

consumer.[1] The Department of Defense (DOD) alone consumes over 29 million megawatt-hours. *Id.*

17. Various statutes and regulations authorize federal agencies to enter into contracts with entities such as CLP for utility services and designate the General Services Administration ("GSA") as the lead federal contracting agency. Utility services include electricity, natural gas, water, sewerage, thermal energy, chilled water, hot water, and steam.

18. The GSA has delegated certain authority to DoD to enter into utility service contracts on behalf of the military departments, and delegated similar authority to other federal agencies. *See* FAR 41.103. The Secretary of a military department can enter into contracts for the conveyance of utility services to private companies like CLP for up to 50 years if it is determined to be cost effective. *See* 10 U.S.C § 2688. The Defense Logistics Agency ("DLA") acts as the executive agent for purchasing fuel and electricity for DoD.

19. Federal agencies may acquire goods and services using multiyear contracts under the authority of the Federal Property and Administrative Services Act of 1949 (Section 304B), as codified in 41 U.S.C. § 254(c). The DoD has similar authority to acquire property using multi-year contracts under 10 U.S.C. § 2306(b). General military laws governing the Armed Forces acquisition process fall under 10 U.S.C. Chapter 137–Procurement.

20. The term "acquisition" means the process of using appropriated funds to contract for the purchase or lease of property or services that support the missions and goals of an executive agency, as defined in 41 U.S.C. § 403 (Public Contracts). The general "procurement" process

[1] *Congressional Research Center Report,* August 15, 2011, Federal Agency Authority to Contract for Electric Power and Renewable Energy Supply found at http://nationalaglawcenter.org/wp-content/uploads/assets/crs/R41960.pdf

includes all the steps agencies take in acquiring property or services, beginning with determining a need for property or services and ending with contract completion and closeout.

21. All federal agencies must follow the Federal Acquisition Regulation ("FAR") system in Title 48 of the Code of Federal Regulations (C.F.R.).[2] Individual federal agencies may also develop their own internal requirements to supplement the FAR System, as have DoD under the Defense Federal Acquisition Regulation System ("DFAR")[3] and the Department of Homeland Security with the Homeland Security Acquisition Regulations ("HSAR").[4]

REGULATIONS REQUIRE SECURING BOTH GOVERNMENT CONTRACTOR INFORMATION SYSTEMS AND THE INFORMATION ON OR PASSING THROUGH THOSE SYSTEMS

A. FAR Rules Require the Protection of Information Systems by Government Contractors.

22. In May of 2016, the federal government announced FAR section 4.19 and clause 52.204-21, which set forth standards for the basic safeguarding of contractor information systems that process, store or transmit federal contract information. These rules finalized proposed revisions to the FAR first published in 2012 and became effective on June 15, 2016.

23. Pursuant to clause 52.204-21, the phrase "Federal contract information" means information, not intended for public release, that is provided by or generated for the government under a contract to develop or deliver a product or service to the government (excluding public information). FAR 52-204.21(a).

---

[2] Title 48 C.F.R.–The Federal Acquisition Regulations System. Also, see P.L. 93-400 Office of Federal Procurement Policy Act of 1974 as amended by P.L. 96-83 Office of Federal Procurement Policy Act, *http://homepage.mac.com/slotcarbob/buchtel69/nowandthen.htmlAmendments* of 1979. Federal Acquisition Regulations are available at http://farsite.hill.af.mil/ VFDFARA.HTM.

[3] See 48 C.F.R. Parts 201 through 299.

[4] The HSAR establishes uniform Department of Homeland Security policies and procedures for all acquisition activities within the Department of Homeland Security. 48 C.F.R. § 3001.301.

24. The breadth of the "Federal contract information" definition captures contractor operational systems. In other words, the regulations apply to virtually all federal contractors and their information systems, with the exception of commercial-off-the-shelf products as defined in FAR 2.101.

25. Pursuant to FAR 52-204.21, as of June 15, 2016, government contractors are required to, among other things: (1) identify, report and correct information and information system flaws and intrusions in a timely manner (within 72 hours); (2) provide protection from malicious code at appropriate locations within organizational information systems; (3) update malicious code protection mechanisms when new releases are available; and (4) perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. *See* FAR 52-204.21(b)(1)(xii)-(xv).

26. The FAR cyber security rules apply to all covered federal contractor information systems, which are systems that are owned or operated by a contractor and that process, store or transmit federal contract information. *See* FAR 52-204.21.

27. "Covered contractor information system" means "an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information." FAR 52.204-21(a).

28. "Information" is defined as "any communication or representation of knowledge in any form, including audiovisual." FAR 52.204-21(a).

29. "Information System" is defined as a "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information." FAR 52.204-21(a).

30. "Safeguarding" is defined as "measures or controls that are prescribed to protect information systems." FAR 52.204-21(a).

31. The phrases "residing and transiting" information and information "residing on" an information system refers to information "being processed by or stored on the information system." 81 Fed. Reg. 30441 (May 16, 2016).

32. Information "transiting through" an information system "means simple transport," as opposed to requiring that the information actually be stored on an information system. *Id.*

33. In brief, the FAR security measures set forth in 52.204-21 are designed to protect the information systems themselves that either contain governmental information or through which governmental information passes - regardless of the content of the information at issue. Cyber security measures designed to protect the information content located on information systems are addressed in detail by the DFAR and HSAR.

B. The Departments of Defense and Homeland Security Require Contractors to Protect the Content of System Information.

34. As relates specifically to the protection of governmental information contained on or passing through a government contractor's information system, this is a more specific issue addressed by the DoD and DHS with their supplementation of the FAR with the DFAR and HSAR. *See e.g.,* DFAR 252.204-7008, HSAR 3052.204-70(a).

35. In brief, the DFAR, among other things, commands government contractors that they must take affirmative steps to protect unclassified information which resides upon or passes through a contractor's electronic data systems in the performance of their contractual duties. More precisely, DFAR 252.204-7008 commands that "[t]he security requirements required by contract clause 252.204-7012, Covered Defense Information and Cyber Incident Reporting, shall be

implemented for all covered defense information on all covered contractor information systems that support the performance of this contract." (emphasis added).

36. Among the security requirements set forth in DFAR 252.204-7012: "[t]he Contractor shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under th[e] contract." 252.204-7012(b). To assure this is accomplished, the section goes on to state ". . . the Contractor shall . . . [i]mplement information systems security protections on all covered contractor information systems including, at a minimum . . . covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government." *Id.* (emphasis added).

37. DFAR 252.204-7012 goes on to provide definitions for classes of information that must be secured by the contractor. These include: (1) "Controlled technical information;" (2) "covered contractor information system;" and (3) "covered defense information." Each of these categories is then further defined by the DFAR under the title, "Safeguarding Covered Defense Information and Cyber Incident Reporting."

38. Pursuant to DFAR 252.204-7012, "[c]ontrolled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination . . . [t]he term does not include information that is lawfully publicly available without restrictions."

39. Pursuant to DFAR 252.204-7012, "[c]overed contractor information system means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information."

40. Pursuant to DFAR 252.204-7012, "[c]overed defense information" includes, among other things, unclassified information that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract, and falls into any one of four categories: (1) Controlled technical information (defined above); (2) Critical Information (operations security); (3) Export Control; or (4) any other information marked or otherwise identified in the contract that requires safeguarding.

41. DFAR 252.204-7012 defines "Critical information (operations security)" as "Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process)."

42. DFAR 252.204-7012 defines "Export control" as "[u]nclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information." (emphasis added).

43. As relates to the "any other information" category, DFAR 252.204-7012 defines this as "[a]ny other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (e.g., privacy, proprietary business information)."

44. DFAR 252.204-7012 goes beyond simply setting forth that government contractors must protect unclassified information, however. DFAR 252.204-7012 goes on to declare certain

actions that must be taken by government contractors in the event that a breach of these security measures is identified. *See* DFAR 252.204-7012(c).

45. Pursuant to DFAR 252.204-7012(c), entitled "Cyber incident reporting requirement," when the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor is required to investigate and report the incident to the DOD within the 72 hour hours. *See* DFAR 252.204-7012(c)-(c)(i). (emphasis added).

46. Much the same as the DFAR provisions outlined above, the Department of Homeland Security ("DHS") supplemented the FAR with additional requirements which relate to those who contract with DHS in the handling of unclassified information as far back as June of 2006. *See* HSAR 3052.204-70.

47. HSAR 3052.204-70(a) states, "[t]he Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission." (emphasis added).

48. Collectively, the FAR, DFAR and HSAR command that government contractors such as CLP take proactive security measures designed to protect not only the information systems containing governmental information, but to protect governmental information itself and report to governmental officials within 72 hours when these measures have failed or have otherwise been

breached. As discussed below, CLP has repeatedly failed or otherwise refused to comply with these security and reporting requirements in relation to seven of its contracts with the United States.

FACTUAL BACKGROUND AND CONDUCT ALLEGED

A. CLP's Functions Under Seven Contracts with the United States by Which It Receives and Retains Government Information on its Information System.

49. CLP began contracting with the United States Government as early as 2010 through a series of contracts to provide electrical infrastructure services, including power distribution, electrical transformers, communications lines and the construction of structures related to these services upon several military installations located throughout the United States. In all, CLP has entered into seven separate but interrelated contracts with the United States between October 23, 2010 and November 20, 2015 for which it has billed and continues to bill the United States.

50. The first contract at issue is contract number HSBP1010C00102. CLP entered into this Contract with the Department of Homeland Security ("DHS"), via U.S. Customs Border and Security, on or about August 23, 2010 to provide electrical power, communications lines and related structures to the March Air Reserve Base located in the State of California. The actual contract between CLP and DHS, however, remains in the exclusive possession and control of CLP.

51. Pursuant to the terms and conditions of HSAR 3052.204-70(a) (effective June, 2006), CLP became responsible for all IT security for their information systems connected to a DHS network or operated by CLP for DHS as early as early as 2010, regardless of location of these systems. As a result, CLP was required to have IT security measures in place to protect the government information contained on every information system operated by CLP which contained information supplied to CLP by DHS so that CLP could perform upon the contract.

52. Upon information and belief, in the performance of its duties under contract HSBP1010C00102, CLP received and retained from DHS certain governmental information

relating to the March Air Reserve Base, and became responsible for maintaining the same, which would place national security at risk were the information systems breached, such as schematics and/or blueprints relating to the size and physical layout of the military base, the location of command structures, the location of power distribution centers and the locations of communications lines.

53. The second contract at issue is contract number SP060008R0804. CLP entered into this contract with Department of the Army ("DOA"), via the Defense Logistics Agency ("DLA"), on or about November 30, 2011 to provide electric power distribution to the Aberdeen Proving Grounds located in the State of Maryland. The actual contract between CLP and DOA remains in the exclusive possession and control of CLP.

54. Pursuant the provisions of FAR 52.204-21 and DFAR 252.204-7012, CLP became contractually obligated to provide adequate security for all covered defense information on CLP's information systems that supported the provision of electrical power to the Aberdeen Proving Grounds, or any other information system operated and maintained by CLP in order to supply electrical power to the Aberdeen Proving Grounds. Moreover, by virtue of CLPs preexisting contract with DHS in relation to the March Air Reserve base in 2010, CLP was required to already have in place cyber security and IT protective measures to secure government information contained on CLP's information systems.

55. Upon information and belief, in the performance of its duties under contract SP06008R0804, CLP received and retained from DOA certain governmental information relating to the Aberdeen Proving Grounds, and became responsible for maintaining the same, which would place national security at risk were the information system breached, such as schematics and/or

blueprints relating to the size and physical layout of the military base, the location of command structures, the location of power distribution centers and the locations of communications lines.

56. The third contract at issue is contract number W912LA12P8034. CLP entered this contract with Department of Defense ("DoD"), via the Department of the Air Force ("DOAF"), on or about November 24, 2012 to provide electrical transformers, electrical power and communications lines, as well as the construction of structures related to these, at the March Air Reserve Base located in the State of California. The actual contract between CLP and DoD remains in the exclusive possession and control of CLP.

57. Pursuant the provisions of FAR 52.204-21 and DFAR 252.204-7012, CLP became contractually obligated to provide adequate security for all covered defense information on CLP's information systems that supported the provision of electrical power to the March Air Reserve Base, or any other information system operated and maintained by CLP in order to supply electrical power to the March Air Reserve Base. Moreover, by virtue of CLPs preexisting contract with DHS in relation to the March Air Reserve base in 2010, CLP was required to already have in place cyber security and IT protective measures to secure government information contained on CLP's information systems.

58. Upon information and belief, in the performance of its duties under contract W912LA12P8034, CLP received and retained from the DOAF certain governmental information relating to the March Air Reserve Base, and became responsible for maintaining the same, which would place national security at risk were the information system breached, such as schematics and/or blueprints relating to the size and physical layout of the military base, the location of command structures, the location of power distribution centers and the locations of communications lines.

59. The fourth contract at issue is contract number SP060009C8270. CLP entered this contract with the DOAF, via the Defense Logistics Agency ("DLA"), on or about May 19, 2014 to provide electric power distribution to Travis Air Force Base located in the State of California. The actual contract between CLP and DOAF remains in the exclusive possession and control of CLP.

60. Pursuant the provisions of FAR 52.204-21 and DFAR 252.204-7012, CLP became contractually obligated to provide adequate security for all covered defense information on CLP's information systems that supported the provision of electrical power to the Travis Air Force Base, or any other information system operated and maintained by CLP in order to supply electrical power to the Travis Air Force Base. Moreover, by virtue of CLPs preexisting contract with DHS in relation to the March Air Reserve base in 2010, CLP was required to already have in place cyber security and IT protective measures to secure government information contained on CLP's information systems.

61. Upon information and belief, in the performance of its duties under contract SP060009C8270, CLP received and retained from DOAF certain governmental information relating to the Travis Air Force Base, and became responsible for maintaining the same, which would place national security at risk were the information system breached, such as schematics and/or blueprints relating to the size and physical layout of the military base, the location of command structures, the location of power distribution centers and the locations of communications lines.

62. The fifth contract at issue is contract number SP060009C8253. CLP entered this contract with the DoD, via DOAF, on or about January 21, 2015 to provide electric power

distribution to the March Air Reserve Base located in the State of California. The actual contract between CLP and DOAF remains in the exclusive possession and control of CLP.

63. Pursuant the provisions of FAR 52.204-21 and DFAR 252.204-7012, CLP became contractually obligated to provide adequate security for all covered defense information on CLP's information systems that supported the provision of electrical power to the March Air Reserve Base, or any other information system operated and maintained by CLP in order to supply electrical power to the March Air Reserve Base. Moreover, by virtue of CLPs preexisting contract with DHS in relation to the March Air Reserve base in 2010, CLP was required to already have in place cyber security and IT protective measures to secure government information contained on CLP's information systems.

64. Upon information and belief, in the performance of its duties under contract SP060009C8253, CLP received and retained from DOAF certain governmental information relating to the March Air Reserve Base, and became responsible for maintaining the same, which would place national security at risk were the information system breached, such as schematics and/or blueprints relating to the size and physical layout of the military base, the location of command structures, the location of power distribution centers and the locations of communications lines.

65. The sixth contract at issue is contract number SP060011C8275. CLP entered this contract with DOA, via DLA, on or about October 23, 2015 to provide electric power distribution to the Aberdeen Proving Grounds located in the State of Maryland. The actual contract between CLP and DOA remains in the exclusive possession and control of CLP.

66. Pursuant the provisions of FAR 52.204-21 and DFAR 252.204-7012, CLP became contractually obligated to provide adequate security for all covered defense information on CLP's

information systems that supported the provision of electrical power to the Aberdeen Proving Grounds or any other information system operated and maintained by CLP in order to supply electrical power to the Aberdeen Proving Grounds. Moreover, by virtue of CLPs preexisting contract with DHS in relation to the March Air Reserve base in 2010, CLP was required to already have in place cyber security and IT protective measures to secure government information contained on CLP's information systems.

67. Upon information and belief, in the performance of its duties under contract SP060011C8275, CLP received and retained from DOA certain governmental information relating to the Aberdeen Proving Grounds, and became responsible for maintaining the same, which would place national security at risk were the information system breached, such as schematics and/or blueprints relating to the size and physical layout of the military base, the location of command structures, the location of power distribution centers and the locations of communications lines.

68. The seventh contract at issue is contract number SP060014C8291. CLP entered this contract with DOAF, via DLA, on or about November 20, 2015 to provide electric power distribution to Hill Air Force Base located in the State of Utah. The actual contract between CLP and DOAF remains in the exclusive possession and control of CLP.

69. Pursuant the provisions of FAR 52.204-21 and DFAR 252.204-7012, CLP became contractually obligated to provide adequate security for all covered defense information on CLP's information systems that supported the provision of electrical power to Hill Air Force Base or any other information system operated and maintained by CLP in order to supply electrical power to Hill Air Force Base. Moreover, by virtue of CLPs preexisting contract with DHS in relation to the March Air Reserve base in 2010, CLP was required to already have in place cyber security and IT protective measures to secure government information contained on CLP's information systems.

70. Upon information and belief, in the performance of its duties under contract SP060014C8291, CLP received and retained from DOAF certain governmental information relating to the Hill Air Force Base, and became responsible for maintaining the same, which would place national security at risk were the information system breached, such as schematics and/or blueprints relating to the size and physical layout of the military base, the location of command structures, the location of power distribution centers and the locations of communications lines.

B. CLP's Failures and Refusals to Comply with the FAR, DFAR and HSAR Commandments to Preserve the Security of the Information and Information Systems Operated on Behalf of the United States.

71. As noted above, Relator began working for CLP as a systems administrator in March of 2016, and continued in that capacity through August 12 of 2016. During those five months, Brooks' duties included examining hardware and software information systems to discover and install necessary updates to avoid cyber intrusion and the intrusion of unwanted software or viruses into the information systems CLP operated and maintained pursuant to the seven contracts with the United States discussed above.

72. As further noted above, because CLP is a government contractor, the FAR, DFAR and HSAR command CLP to not only take proactive measures to protect the information systems it operates on behalf of the government, but that CLP act to protect government information contained on its information systems – including reporting to the government, within 72 hours, when CLP's efforts had failed or were otherwise compromised.

73. Shortly after he began working for CLP, Relator learned that CLP surprisingly employs no permanent IT professional to monitor CLP's information systems. Rather, CLP contracts with a third-party company, Timberlan, to provide CLP's IT security services. CLP then supplements Timberlan's services from time to time with on-site contractors such as Relator.

74. Through the performance of his duties for CLP, however, Relator discovered that CLP is failing or otherwise refusing to comply with the commands of the FAR, DFAR and HSAR in two primary ways. First, CLP is failing to properly maintain, update and secure its information and information systems operated for the United States or containing information conveyed by the United States. Second, CLP is failing to notify the government of the breach of its information systems within 72 hours of a breach event.

75. By way of example of CLP's continued and repeated failures, Relator notes that on or about April 14, 2016, he logged into CLP's system security software's (Bitfender) control panel and discovered that approximately 90% of CLP's employee computers were not being updated at all. Relator immediately reported this security issue to his supervisor, Brad Weber, in an email of April 15, 2016, entitled "Computer vulnerability." *Attached hereto as Exhibit* 1. By that correspondence, Relator advised Mr. Weber that numerous CLP computers were not equipped with anti-virus software- a condition exposing CLP's entire information system to exploitation. *See id.*

76. Another example of CLP's continued security failures was demonstrated on or about May 1, 2016 when Relator discovered that it was not just individual computers and computer systems that were vulnerable, but that CLP's entire host of servers was vulnerable to exploitation for want of system security and software updates. Again, Relator immediately raised this security issue with Mr. Weber. Mr. Weber explained that Relator's IT predecessor at CLP had turned off the automated updates throughout the information system in order to enable himself to manually select which updates to install, when to install these and whether these updates would be installed at all. Relator protested, explaining that the missing updates were important to the integrity and security of the entire information system, even critical in many instances.

77. Another example of CLP's repeated information system security failures is memorialized in an email from Kevin Umphress of May 12, 2016 wherein Mr. Umphress advised all employees of CLP's Denver office of the need to log out of the information system no later than 4:45 p.m. on that day so that Relator could perform a necessary server update. *Attached hereto as Exhibit* 2. This server update was necessitated by Brad Weber's instruction to Relator to solve those system security issues he discovered.

78. CLP's repeated security failures are further exemplified in a series of emails from mid- May of 2016 through mid- August of 2016. For instance, by correspondence of May 16, 2016, CLP employee Rachel Vonsiebenhoven forwarded Relator an email from a cyber hacker. *Attached hereto as Exhibit* 3. This email "spoofed" the email of the President of CLP, Tom Simmons, inquiring as to whether Ms. Vonsibenhoven was in the office because he wanted her to process an urgent payment to a new vendor. *Id.* Tom Simmons later confirmed that he had not sent the email. In brief, Relator's cyber security concerns had become manifest. It was no longer only possible that CLP's security failures could result in a breach of its information systems; CLP's information systems had already been breached to such an extent that he hacker knew the relative positions of CLP employees and who to target in an effort to receive fraudulent payments. *See id.*

79. On May 17, 2016, in response to the Vonsiebehoven incident, in an email string entitled "IT Security Violation," Relator tracked down and contacted the hacker's email provider to advise of the cyber intrusion and hacking concern. *Attached hereto as Exhibit* 4. In light of his knowledge of these events, as well as his knowledge that CLP provided various electrical power services to U.S. military installations and maintained information relating to U.S. Military installations on it information systems, Relator began to research government regulations relating to cyber security.

80. On May 28, 2016, in an email string entitled "server updated," Relator specifically drew his supervisor's attention to the fact that one particular server had never been updated at all. *Attached hereto as Exhibit* 5.

81. A June 15, 2016 email string forwarded to Relator from Rachel Vonsiebehoven from Baker, Tilly, Virchow, Krause, LLP[5] entitled "New Cybersecurity Requirements for Government Contractors," states, "[e]ffective today, a new rule published by the U.S. Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) will require Federal Government contractors to apply 15 basic cybersecurity safeguarding requirements and procedures to protect their information systems. The new rule specifically applies to covered contractor information systems used to process, store, or transmit federal contract information, and most contractors are expected to be impacted by the rule." *Attached hereto as Exhibit* 6.

82. On or about June 20, 2016, Relator conducted a weekly meeting with Mr. Weber to discuss Relator's work load. During that meeting, Relator advised Mr. Weber of the seriousness of the Vonsibenhoven incident and the security concerns posed to the entire CLP information system.

83. On June 29, 2016, in an email entitled, "phone outage," Relator advised Mr. Weber that CLP's telephone system, a Shoretel telephone server system, had 195 updates waiting to be implemented. *Attached hereto as Exhibit* 7. This reality did not just leave CLP's entire telephone system vulnerable to exploitation; inasmuch as the vast majority of CLP's computers were connected to the information system via a telephone port, each such computer was equally

[5] Baker Tilly, LLP is a full-service accounting and advisor firm offering industry specialized services in audit, tax and management consulting.

vulnerable to exploitation. In other words, every component of CLP's information system connected via a telephone port was vulnerable to exploitation and cyber intrusion.

84. On June 29, 2016, CLP appeared to acknowledge the security threat posed by its previous failures. More precisely, by an email string of that date entitled, "Hacking_Spoofing_Phishing," CLP employee Rachel Vonsiebehoven established a cyber security training class for CLP's accounting department as a result of the cyber security scare created from the Vonsibenhoven incident. *Attached hereto as Exhibit* 8.

85. On July 5, 2016, in an email string entitled "Questions," Relator was instructed by Mr. Weber to determine why the Shoretel phone server had not been updated. *Attached hereto as Exhibit* 9.

86. On or about July 6, 2016, the owner of Timberlan, Eric Bradac, advised Relator that it was standard procedure for Shortel specific companies to stick with a stable platform once one had been established. *Attached hereto as Exhibit* 9. Nevertheless, Relator contacted Shortel representative Travis Bitzer on that same date and was advised that this was incorrect and the 195 updates needed to be immediately implemented to assure the integrity of the telephone system.

87. On July 13, 2016, Relator ordered a free network threat check device from a company called Computer Discount Warehouse, or CDW. Relator then installed a security protocol (Spiceworks) onto the information system on July 19, 2016, designed to inventory all devices attached to CLP's information system, create a network map, monitor suspicious connection attempts and notify him of possible information system intrusion attempts.

88. From July 19, 2016 to August 11, 2016, Relator was notified of twenty separate information system intrusion alerts that appeared to be increasing in frequency. As a result, Relator began forwarding notifications to Mr. Weber.

89. On July 21, 2016, Relator forwarded to Mr. Weber a notice of a suspicious attempted intrusion into CLP's information system. *Attached hereto as Exhibit* 10. By that notice, entitled, "Suspicious IP 212.83.174.199 attempted to connect to clpex01 (Central Server). View Threat Details," Relator advised Mr. Weber that attempted intrusions were occurring and a conversation was needed to discuss the prevention of cyber-attacks on CLP's information systems. *Id.* Mr. Weber merely advised that he did not have time to deal with the issue and that Relator should do whatever Relator or others determined needed to be done. *Id.*

90. On July 26, 2016, Relator advised CLP President Bill Simmons that CLP information system computers are not set to automatic updates and that there had been successful cyber intrusions into CLP's information system. *Attached hereto as Exhibit* 11.

91. On August 2, 2016, Relator installed a system threat scan device to CLP's information system and initiated the scan. The scan was scheduled to be completed on August 19, 2016 and was intended to examine CLP's entire information system.

92. On August 5, 2016, Relator was advised by CLP employee Megan Bleess of a potential data breach in CLP's Cartopac project and that a third-party employee vendor was accessing CLP's server in an unmonitored fashion. Relator immediately contacted the site manager for the project, Barbra Ely, to request information relating to the potential security breach. Relator received those details via email on August 5, 2016 and immediately discussed the security breach with Mr. Weber. *Attached hereto as Exhibit* 13. During that conversation, Relator advised Mr. Weber that government regulations required, among other things, that the security issue needed to be reported to the government within 72 hours. *See attached Exhibit* 12. Upon information and belief, neither this incident, nor any other event of cyber intrusion, was ever reported to any of the contracting governmental entities.

93. On August 10, 2016, Relator spoke with Mr. Weber in Mr. Weber's office relating to the importance of governmental cyber security regulations. Mr. Weber advised Relator that "if no one is around to catch you jaywalking or speeding 5 mph over the speed limit what's going to happen?" This conversation was memorialized in correspondence from Relator to Mr. Weber in an email of August 11, 2016. *Attached hereto as Exhibit* 14. By that correspondence, Relator further advised Mr. Weber of the need to conduct an investigation into suspected cyber breaches into CLP's information system." *Id.* Weber simply requested that Relator drop the issue. *Id.*

94. An email string dated August 12, 2016, entitled "server issues," demonstrates that an update service was running on a server which served to "push out updates" to the desktop and laptop computers on CLP's information system. *Attached hereto as Exhibit* 15. Part of this "push" contained system updates that had been waiting to be performed since 2013. This was Brooks' last day of employment with CLP.

95. On or about August 15, 2016, Relator was advised by Megan Bleess that Timberlan began the process of removing the updates performed by Relator in CLP's information systems after his departure. Ms. Bleess further advised Relator that Timberlan had removed the network monitoring protocol that Relator had installed on the information system known as the "Spiceworks ticketing system."

96. Relator's information system security concerns were only bolstered throughout his time at CLP by discussions with CLP personnel.

97. Over the course of his employment with CLP, Relator had repeated conversations with Megan Bleess, the ARCGIS Administrator of Engineering for CLP, relating to Timberlan's numerous failures to assure the security of CLP's information system. In one particular instance,

Ms. Bleess advised Relator of Timberlan's refusal to supply her with something as simple as a website security certificate- a feature required to assure the security of CLP's information system.

98. Relator additionally spoke with Ken Ganskow, the former safety director for CLP, on or about August 14, 2016. During that conversation, Mr. Ganskow advised Relator that he left the company because CLP attempted to compel Mr. Ganskow to falsify safety numbers that were to be reported to OSHA.

99. On or about August 15, 2016, Relator spoke with Kimberly Herivel, the former media advisor for CLP. While Relator cannot recall the specifics of that conversation, he was advised by Ms. Herivel that she was aware that CLP was failing to comply with numerous information system security regulations and other such regulations.

100. Relator also spoke with Anastasia Shippey on or about August 15, 2016, the former regulations analyst for CLP. Ms. Shippey advised Relator of the existence of an email conversation with the President of CLP wherein information system security regulations were discussed but ultimately disregarded by CLP.

101. It is from these observations and conversations during his time as an employee with CLP that Relator discovered that CLP is not complying with the information and information system security and reporting commands of the FAR, DFAR and HSAR. From these known and continuing failures, Relator now brings these claims, on behalf of the United States, for past and continuing violations of the False Claims Act.

FIRST CLAIM FOR RELIEF
Violations of the False Claims Act - 31 U.S.C. § 3729(a)(1)(A) and (B)

102. Relator hereby incorporates by reference each all of the preceding paragraphs of this Complaint as though fully set forth herein in their entirety.

103. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. § 3729 et seq., as amended.

104. By virtue of the acts described above, CLP, through its agents and employees, knowingly presented or caused to be presented false or fraudulent claims, certifications, records and/or other materials for payment and/or approval which resulted in countless millions of dollars of payments of false claims by the United States government to CLP. All such false claims and acts are in violation of the FCA in general and specifically in violation of 31 U.S.C. § 3729(a)(1)(A), as amended.

105. Additionally, by virtue of the acts described above, the Defendants knowingly made, used or caused to be made or used, false records, certifications and statements material to a false or fraudulent claim which resulted in millions of dollars of payments of false claims by the United States Government to CLP. All such false claims and acts are in violation of the FCA in general and specifically in violation of 31 U.S.C. § 3729(a)(1)(B), as amended.

106. The acts described above induced the United States Government to pay or approve such false or fraudulent claims.

107. Every such payment by the United States to CLP for goods, materials and/or services that were certified and/or represented to be made available to the government in accordance with the information systems and security provisions of the FAR, DFAR and HSAR, and the numerous contractual requirements for eligibility and receipt of payment were the product of a false claim, certification and materially false statements made by CLP.

108. Because of its fraudulent conduct, the CLP is and was ineligible for payments because CLP, with knowledge and design, was not and is not in compliance with the Act, regulations, FAR, DFAR, HSAR or contractual provisions existing as a prerequisite for payment.

109. In reliance on these false representations, certifications and claims, the United States Government, by and through its intermediaries, paid countless millions of dollars for products and services that it otherwise would not have purchased from CLP had the government been aware of CLP's knowing violations of the FCA and the various rules and regulations relating to the security and maintenance of information and information systems operated and maintained pursuant to government contracts paid for with federal monies.

110. By reason of CLP's acts, the United States has been damaged and continues to be damaged in substantial amounts to be determined at trial.

111. Pursuant to the FCA, CLP is liable to the United States for a civil penalty of not less than $5,500 and not more than $11,000 for each of the false or fraudulent claims and certifications made, plus three times the amount of damages which the United States has sustained because of CLP's actions and inactions.

SECOND CLAIM FOR RELIEF
Violations of the False Claims Act 31 U.S.C. § 3729(a)(1)(C) – Conspiracy

112. Relator hereby incorporates by reference each and all of the preceding paragraphs of this Complaint as though fully set forth herein in their entirety.

113. CLP, through its agents and employees, has conspired to win contracts, or participate in the same as suppliers of materials, goods and services with the United States Government through a series of fraudulent and false misrepresentations and certifications in relation to services and practices to be observed and performed, all in violation of the FCA as set forth above in 31 U.S.C. § 3729(a)(1)(c).

114. In furtherance of the conspiracy, the Defendant-conspirators agreed to present false certifications, records and/or statements to the United States that would have a material effect on

the United States Government's decision to pay for the contested items and services referenced herein.

115. The Defendant-conspirators intentionally or knowingly made false certifications and statements to various federal agencies and/or caused others to submit false certifications and statements to various federal agencies, and failed to report information system cyber intrusions to the United States, all in order to lead the United States to believe that the information supplied to CLP, and information systems containing and/or receiving such information, was/were secure and/or would be secured under circumstances in which CLP had not secured and was not securing such government information or information systems, all the while seeking and continuing to seek payment from the United States.

116. By reason of CLP's actions and inactions, the United States has been damaged and continues to be damaged in substantial amounts to be determined at trial.

117. Pursuant to the FCA, CLP is liable to the United States for a civil penalty of not less than $5,500 and not more than $11,000 for each of the false or fraudulent claims and certifications herein, plus three times the amount of damages which the United States has sustained because of CLP's actions.

SUMMARY

118. As alleged herein and above, CLP bid upon and ultimately was awarded numerous governmental contracts for the supply and maintenance of electrical distribution and infrastructure services and supplies to U.S. military installations. Pursuant to various provisions of the Federal Acquisition Regulation, Defense Federal Acquisition Regulation and the Homeland Security Acquisition Regulation, CLP was commanded to undertake certain security measures to safeguard government information received from governmental entities and to timely report to government

officials breaches of these required security measures. Nevertheless, CLP has knowingly, willfully and repeatedly failed or otherwise refused to undertake these required security and reporting requirements while continuing to create and submit claims to the government for payment and approval, and upon which the government has and continues to make payment. For these actions and inactions, CLP is now liable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, the United States of America, through Relator Jeffrey Brooks, hereby requests the Court for entry of judgment against Defendant and the following relief:

A. That CLP cease and desist from further violations of the False Claims Act, 31 U.S.C. § 3729 *et seq.*;

B. That the Court enter judgment against CLP in an amount equal to three times the amount of damages suffered by the United States because of CLP's actions and inactions, plus a civil penalty of not less than $5,500 and not more than $11,000 for each false claim and certification;

D. That Relator Brooks be awarded the maximum amount allowed pursuant to section 3730(d) of the False Claims Act, as well as the reasonable costs and attorney's fees associated with brining this action; and

G. That the United States and Brooks be granted such further relief as the court deems equitable, just and proper.

JURY DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, a jury trial is demanded.

Respectfully submitted on this 9th day of November, 2016.

By:

DAVID P. WEBER, Bar No. 07225
RICHARD J. LINK, Bar No. 24465
GOODWIN WEBER PLLC
Attorneys for Plaintiff-Relator
Local Counsel
267 Kentlands Blvd., Suite 250
Gaithersburg, MD 20878
(301) 850-3370
(301) 850-3374 FAX
David.Weber@goodwinweberlaw.com

/s/ Brian H. Mahany

Brian H. Mahany
Mahany Law
Pro Hac Vice Anticipated
8112 West Bluemound Road
Suite 101
Wauwatosa, Wisconsin 53213
Office: (414) 258-2375
Email: brian@mahanylaw.com
Attorney for Plaintiff-Relator